МИНИСТЕРСТВО ОБРАЗОВАНИЯ РЕСПУБЛИКИ БЕЛАРУСЬ

Учебно-методическое объединение по естественнонаучному образованию

УТВЕРЖДАЮ
Первый заместитель Министра образования Республики Беларусь
_____ В.А.Богуш
«20» 05 2015г.
Регистрационный № ТД-Р601/тип.

КРИПТОГРАФИЧЕСКИЕ МЕТОДЫ

Типовая учебная программа по учебной дисциплине для направления специальности 1- 98 01 01- 01 Компьютерная безопасность (математические методы и программные системы)

СОГЛАСОВАНО
Председатель Учебно-методического объединения по естественнонаучному образованию
_____ А.Л. Толстик
28 _____ 2015 г.

СОГЛАСОВАНО
Начальник Управления высшего образования Министерства образования Республики Беларусь
_____ С.И. Романюк
«20» 05 2015 г.

СОГЛАСОВАНО
Проректор по научно-методической работе Государственного учреждения образования «Республиканский институт высшей школы»
_____ И.В. Титович
«05» 05 2015 г.

Эксперт-нормоконтролер
_____ А.А.Денисевич
«28» 04 2015 г.

Минск 2015

СОСТАВИТЕЛИ:
С.В. Агиевич, доцент кафедры математического моделирования и анализа данных Белорусского государственного университета, кандидат физико-математических наук
И.А. Бодягин, доцент кафедры математического моделирования и анализа данных Белорусского государственного университета, кандидат физико-математических наук

РЕЦЕНЗЕНТЫ:
Кафедра защиты информации Учреждения образования «Белорусский государственный университет информатики и радиоэлектроники»
В.И. Берник, главный научный сотрудник отдела теории чисел Института математики Национальной академии наук Беларуси, доктор физико-математических наук, профессор

РЕКОМЕНДОВАНА К УТВЕРЖДЕНИЮ В КАЧЕСТВЕ ТИПОВОЙ:
Кафедрой математического моделирования и анализа данных Белорусского государственного университета
(протокол № 17 от 15 апреля 2014 г.);

Научно-методическим советом Белорусского государственного университета
(протокол № 5 от 15 мая 2014 г.);

Научно-методическим советом по компьютерной безопасности учебно-методического объединения по естественнонаучному образованию
(протокол № 7 от 22 апреля 2014г.).

Ответственный за редакцию: И.А. Бодягин

Ответственный за выпуск: И.А. Бодягин

Пояснительная записка

Типовая учебная программа по учебной дисциплине «Криптографические методы» разработана в соответствии с типовым учебным планом и образовательным стандартом первой ступени высшего образования для направления специальности 1- 98 01 01- 01«Компьютерная безопасность (математические методы и программные системы)»

Криптографические методы защиты информации обеспечивают конфиденциальность, контроль целостности и проверку подлинности данных с помощью ключезависимых или бесключевых криптографических преобразований.

Учебная дисциплина «Криптографические методы» знакомит студентов с методами построения криптографических преобразований, а также методами оценки их надежности. Кроме того данная учебная дисциплина дает представление об основных типах криптографических систем: блочных, поточных, криптосистемах с открытым ключом, систем электронной цифровой подписи, функций хэширования.

Изучаемые криптографические методы основываются на использовании объектов и применении методов широкого набора математических дисциплин: алгебры, теории чисел, теории вероятностей, математической статистики, теории информации, теории сложности.

Основой для изучения учебной дисциплины «Криптографические методы» являются учебные дисциплины «Геометрия и алгебра», «Дискретная математика и математическая логика», «Теория вероятностей и математическая статистика» государственного компонента, «Математический анализ», «Теория информации» компонента учреждения высшего образования. Сведения, излагаемые в учебной дисциплине «Криптографические методы» используются учебными дисциплинами «Теоретические основы информационной безопасности», «Программно–аппаратные и технические средства защиты информации» государственного компонента, а также при изучении ряда учебных дисциплин специализации.

Цели преподавания учебной дисциплины «Криптографические методы»: во-первых, дать студентам теоретические основы построения надежных криптографических преобразований, и, во-вторых, сформировать навыки использования криптографических преобразований для построения систем защиты информации.

При изложении материала учебной дисциплины важно показать возможности использования конкретных криптографических методов при решении прикладных задач защиты информации.

Основные задачи, решаемые при изучении учебной дисциплины «Криптографические методы»:

– изучение криптосистем с секретным ключом, применение блочных и поточных криптосистем для решения практических задач в области защиты информации;

– изучение криптосистем с открытым ключом, применение функций хеширования для решения задач проверки целостности сообщений, использование ЭЦП;

– изучение основ применения эллиптических кривых в криптографии.

В результате изучения учебной дисциплины студент должен:

знать:

- методы построения надежных блочных и поточных криптосистем, функций хэширования, криптосистем с открытым ключом и систем электронной цифровой подписи;
- задачи и основные методы криптоанализа;
- стандартные криптосистемы и их практическое использование.

уметь:

- применять полученные знания для создания надежных систем защиты информации;

владеть:

- методами построения надежных криптосистем и функций хэширования;
- методами построения криптосистем с открытым ключом и систем электронной цифровой подписи;
- основными методами криптоанализа.

Типовая учебная программа рассчитана на 208 учебных часов, из них 136 аудиторных часов, примерное распределение которых по видам занятий включает: лекции – 68 часов, лабораторные занятия – 34 часа, практические занятия – 34 часа.

Рекомендуемая форма текущей аттестации – экзамен, зачеты.

В соответствии с требованиями образовательного стандарта по специальности 1-98 01 01 «Компьютерная безопасность (по направлениям)» специалист должен владеть следующими академическими компетенциями (АК), социально-личностными (СЛК) и профессиональными компетенциями (ПК):

АК-1. Уметь применять базовые научно-теоретические знания для решения теоретических и практических задач.

АК-2. Владеть системным и сравнительным анализом.

АК-3. Владеть исследовательскими навыками.

АК-4. Уметь работать самостоятельно.

АК-5. Быть способным порождать новые идеи (обладать креативностью).

АК-6. Владеть междисциплинарным подходом при решении проблем.

АК-9. Уметь учиться, повышать свою квалификацию в течение всей жизни.

СЛК-3. Обладать способностью к межличностным коммуникациям.

ПК-1. Работать с научной, нормативно-справочной и специальной литературой с целью получения последних сведений о новых методах защиты информации, о стойкости существующих систем защиты информации.

ПК-2. Формулировать задачи, возникающие при организации защиты информации.

ПК-3. Разрабатывать модели явлений, процессов или систем при организации защиты информации.

ПК-4. Выбирать необходимые методы исследования, модифицировать существующие, разрабатывать новые методы и применять их для решения поставленных задач при организации защиты информации.

ПК-5. Выполнять оценку эффективности методов защиты информации.

ПК-7. Владеть методами и средствами организации работ малых коллективов исполнителей для достижения поставленных целей.

ПК-9. Анализировать и оценивать собранные данные.

ПК-10. Вести переговоры, разрабатывать контракты с другими заинтересованными участниками.

ПК-11. Готовить доклады и материалы к презентациям.

ПК-15. Организовывать процесс создания, оценки и эксплуатации средств и систем защиты информации, поддерживать и повышать их безопасность; осуществлять контроль за их использованием.

ПК-17. Находить оптимальные проектные решения.

ПК-18. Разрабатывать программные, аппаратно-программные и технические средства и системы защиты информации; разрабатывать необходимую документацию.

ПК-19. Выполнять оценку безопасности реализации средств и систем защиты информации.

ПК-21. Эксплуатировать программные, аппаратно-программные и технические средства и системы защиты информации; осуществлять контроль за их использованием; вести необходимую для этого документацию.

ПК-23. Определять цели инноваций и способы их достижения.

Примерный тематический план

	№ темы	**Количество аудиторных часов**		
	Содержание	**Лекции**	**Лабораторные занятия**	**Практические занятия**
	Раздел I. Криптография с секретным ключом			
1.	Введение в криптографию	4		
2.	Классические криптосистемы	2		2
3.	Элементы теории Шеннона	2		2
4.	Элементы теории конечных полей	6		2
5.	Булевы функции в криптографии	2	6	2
6.	Блочные криптосистемы	10	8	4
7.	Свойства линейных рекуррентных последовательностей	2		2
8.	Поточные криптосистемы	6		2

	Раздел II. Криптография с открытым ключом			
9.	Протокол Диффи – Хэллмана	2		2
10.	Элементы теории сложности	2		
11.	Односторонние функции	4		
12.	Криптосистемы с открытым ключом	4	4	4
13.	Генерация простых чисел	2	4	2
14.	Функции хэширования	6	4	2
15.	Электронные цифровые подписи	4	4	2
16.	Факторизация и дискретное логарифмирование	6	2	2
17.	Эллиптические кривые в криптографии	4	2	4
	Всего	68	34	34

Содержание учебного материала

Раздел I. Криптография с секретным ключом

1. Введение в криптографию

История криптографии. Абоненты, коммуникации и угрозы. Задачи криптографии и криптоанализа. Криптосистемы (шифрсистемы). Типы атак. Сложность атак.

2. Классические криптосистемы

Шифр сдвига. Аффинный шифр. Шифр простой замены. Шифр Хилла. Шифр перестановки. Шифр Виженера.

3. Элементы теории Шеннона

Совершенные криптосистемы. Энтропия, условная энтропия, удельная энтропия. Расстояние единственности.

4. Элементы теории конечных полей

Подполя и расширения полей. Характеристика поля. Существование конечного поля. Единственность конечного поля. Соотношения между подполями. Функция следа. Мультипликативная группа конечного поля.

5. Булевы функции в криптографии

Булевы функции и отображения. Преобразование Мебиуса. Преобразование Уолша – Адамара. Нелинейность. *S*-блоки.

6. Блочные криптосистемы

Блочно-итерационные криптосистемы. SP-криптосистемы. AES. Использование инволютивных подстановок. Криптосистемы Фейстеля. Атака «грубой силой». Баланс «время – память». Таблицы разностей. Разностная атака. Конструкция Нюберг. Линейные аппроксимации.

Линейная атака. Режим простой замены. Режим счетчика. Режим цепной обработки. Режим гаммирования с обратной связью.

7. Свойства линейных рекуррентных последовательностей

Порядок многочлена. Примитивные многочлены. Период л.р.п. Минимальный многочлен. Постулаты Голомба.

8. Поточные криптосистемы

Конечные автоматы. Регистры сдвига с линейной обратной связью. Фильтрующий генератор. Комбинирующий генератор. Генератор с неравномерным движением. Криптосистема A5/1. Сжимающий и самосжимающий генератор. Линейная сложность. Корреляционный криптоанализ. Корреляционно-иммунные функции.

Раздел II. Криптография с открытым ключом

9. Протокол Диффи – Хеллмана

Идея криптографии с открытым ключом. Головоломки Меркля. Протокол Диффи – Хеллмана. Реализация протокола Диффи – Хеллмана.

10. Элементы теории сложности

Вычислительные проблемы. Машины Тьюринга. Предикаты. Сложностные классы. Вероятностные машины. Алгоритмы типа Монте-Карло и Лас-Вегас.

11. Односторонние функции

Определение. Функция Рабина. Функции с лазейкой. Лазейка функции Рабина. Функция RSA. Функция Эль-Гамаля.

12. Криптосистемы с открытым ключом

Использование функций с лазейкой для построения криптосистем с открытым ключом. Криптосистема RSA. RSA и факторизация. Реализация: арифметика больших чисел, алгоритм Евклида, возведение в степень, оптимизация RSA.

13. Генерация простых чисел

Язык PRIMES. Проверка простоты. Тесты Ферма и Миллера – Рабина. Построение простых. Теорема Диемитко.

14. Функции хэширования

Определения и задачи криптоанализа. Использование. Генераторы псевдослучайных чисел на базе функций хэширования. Ключезависимые функции хэширования. Блочно-итерационные функции хэширования. Функция хэширования СТБ 34.101.31. Атака «дней рождения». Алгоритм Брента.

15. Электронные цифровые подписи

Использование функций с лазейкой для построения систем ЭЦП. ЭЦП ЭльГамаля. Реализация ЭЦП ЭльГамаля. ЭЦП Шнорра. Система ЭЦП СТБ 1176.2.

16. Факторизация и дискретное логарифмирование

Алгоритм p – 1. ρ-методы. Выбор модуля RSA. Метод больших-малых шагов. λ-метод. Метод Поллига – Хеллмана. Алгоритм Диксона. Квадратичное решето. Индекс-метод.

17. Эллиптические кривые в криптографии

Основные понятия. Сложение точек. Кривые над конечными полями. Кратная точка. ЭЦП Шнорра на эллиптических кривых. Система ЭЦП СТБ 34.101.45

Информационно-методическая часть

Литература

Основная

1. Алферов А. П., Зубов А. Ю., Кузьмин А. С., Черемушкин А. В. Основы криптографии. — Москва: Гелиос АРВ, 2001. — 480 с.
2. Бабаш А. В., Шанкин Г. П. Криптография. Аспекты Защиты. — Москва: Солон–Р, 2002. — 512 с.
3. Харин Ю. С., Берник В. И., Матвеев Г. В., Агиевич С. В. Математические и компьютерные основы криптологии. — Минск: Новое знание, 2003. — 320 с.
4. Харин Ю.С., Агиевич С.В. Компьютерный практикум по математическим методам защиты информации. — Минск, БГУ, 2001. — 190 с.

Дополнительная

1. Menezes A.J., van Oorschot P. C., Vanstone S.A. Handbook of Applied Cryptography. — CRC Press, 1996. — 816 p.
2. Schneier B. Applied Cryptography: Protocols, Algorithms, and Source code in C. — John Wiley & Sons, 1996. — 675 p.
3. Stinson D. Cryptography. Theory and Practice. – N.Y. CRC, 1995 — 434 p.

Диагностика компетенций студента

Условия для самостоятельной работы студентов, в частности, для развития навыков самоконтроля, способствующих интенсификации учебного процесса, обеспечиваются наличием и полной доступностью электронных (и бумажных) учебно-методических пособий по основным разделам дисциплины.

Текущий контроль усвоения знаний рекомендуется осуществлять в виде проверки лабораторных работ, контрольных работ, проведения коллоквиумов.

Рекомендуемая форма текущей аттестации – экзамен, зачеты.